CHAPTER 3

Configuring AnyConnect Features Using the CLI

The security appliance automatically deploys the Cisco AnyConnect VPN client to remote users upon connection. The initial client deployment requires end-user administrative rights. The AnyConnect client supports the HTTPS/TCP (SSL) and Datagram Transport Layer Settings (DTLS) tunneling options. This chapter describes how to use ASDM to configure AnyConnect features.

You configure the AnyConnect client features on the security appliance, as described in the following sections:

Enabling the SSL VPN Client Protocol

The AnyConnect client uses the SSL VPN protocol, therefore you must enable the SSL VPN Client protocol as part of the configuration process. To do this, use the **svc enable** command in webvpn configuration mode.

Configuring the Login Page Setting

To allow the user to select a connection profile, identified by its alias, on the login page, use the **tunnel-group-list enable** command in webvpn configuration mode. If you do not configure this feature, the AnyConnect client uses the DefaultWebVPNGroup profile as the connection profile.

To specify an alias for a connection profile, use the **group-alias enable** in tunnel-group webvpn-attributes configuration mode.

Enabling Datagram Transport Layer Security (DTLS) with AnyConnect (SSL) Connections

Datagram Transport Layer Security avoids latency and bandwidth problems associated with some SSL-only connections, including AnyConnect connections, and improves the performance of real-time applications that are sensitive to packet delays. DTLS is a standards-based SSL protocol that provides a low-latency data path using UDP. For detailed information about DTLS, see RFC 4347 (http://www.ietf.org/rfc/rfc4347.txt).

Datagram Transport Layer Security (DTLS) allows the AnyConnect client establishing an SSL VPN connection to use two simultaneous tunnels—an SSL tunnel and a DTLS tunnel. Using DTLS avoids latency and bandwidth problems associated with some SSL connections and improves the performance of real-time applications that are sensitive to packet delays.

If you do not enable DTLS, SSL VPN connections connect with an SSL VPN tunnel only.

Enabling DTLS Globally for a Specific Port

To enable DTLS globally for a particular port, use the **dtls port** command:

[no] dtls port *port_number*

The following example enters group policy webvpn configuration mode and specifies port 444 for DTLS:

```
hostname(config)# webvp4
hostname(config-webvpn)# dtls port 445
```

Enabling DTLS for Specific Groups or Users

To enable DTLS for specific groups or users, use the **svc dtls enable** command in group policy webvpn or username webvpn configuration mode:

[**no**] **svc dtls enable**

If DTLS is configured and UDP is interrupted, the remote user's connection automatically falls back from DTLS to TLS. The default is enabled; however, DTLS is not enabled by default on any individual interface.

Enabling DTLS allows the AnyConnect client establishing an AnyConnect VPN connection to use two simultaneous tunnels—an SSL tunnel and a DTLS tunnel. Using DTLS avoids latency and bandwidth problems associated with some SSL connections and improves the performance of real-time applications that are sensitive to packet delays.

If you do not enable DTLS, AnyConnect client users establishing SSL VPN connections connect only with an SSL VPN tunnel.

The following example enters group policy webvpn configuration mode for the group policy *sales* and enables DTLS:

```
hostname(config)# enable inside
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# svc dtls enable
```

Prompting Remote Users

You can enable the security appliance to prompt remote AnyConnect VPN client users to download the client with the **svc ask** command from group policy webvpn or username webvpn configuration modes:

[**no**] **svc ask** {**none** | **enable** [**default** {**webvpn** | **svc**} **timeout** *value*]}

svc ask enable prompts the remote user to download the client or go to the WebVPN portal page and waits indefinitely for user response.

svc ask enable default svc immediately downloads the client.

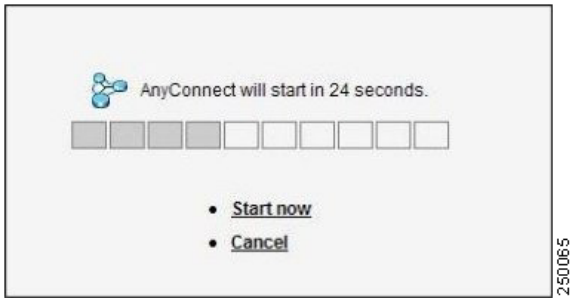
svc ask enable default webvpn immediately goes to the portal page.

svc ask enable default svc timeout *value* prompts the remote user to download the client or go to the WebVPN portal page and waits the duration of *value* before taking the default action—downloading the client.

svc ask enable default webvpn timeout *value* prompts the remote user to download the client or go to the WebVPN portal page, and waits the duration of *value* before taking the default action—displaying the WebVPN portal page.

Figure 3-1 shows the prompt displayed to remote users when either **default svc timeout** *value* or **default webvpn timeout** *value* is configured:

Figure 3-1 Prompt Displayed to Remote Users for SSL VPN Client Download



The following example configures the security appliance to prompt the remote user to download the client or go to the WebVPN portal page and to wait 10 seconds for user response before downloading the client:

```
hostname(config-group-webvpn)# svc ask enable default svc timeout 10
```

Enabling IPv6 VPN Access

The AnyConnect client allows access to IPv6 resources over a public IPv4 connection (Windows XP SP2, Windows Vista, Mac OS X, and Linux only). You must use the command-line interface to configure IPv6; ASDM does not support IPv6.

You enable IPv6 access using the **ipv6 enable** command as part of enabling SSL VPN connections. The following is an example for an IPv6 connection that enables IPv6 on the outside interface:

```
hostname(config)# interface GigabitEthernet0/0
hostname(config-if)# ipv6 enable
```

To enable IPV6 SSL VPN, do the following general actions:

1. Enable IPv6 on the outside interface.
2. Enable IPv6 and an IPv6 address on the inside interface.
3. Configure an IPv6 address local pool for client assigned IP Addresses.
4. Configure an IPv6 Tunnel default gateway.

To implement this procedure, do the following steps:

Step 1 Configure Interfaces:

```
interface GigabitEthernet0/0
     nameif outside
     security-level 0
     ip address 192.168.0.1 255.255.255.0
     ipv6 enable           ; Needed for IPv6.
    !
interface GigabitEthernet0/1
     nameif inside
     security-level 100
     ip address 10.10.0.1 255.255.0.0
     ipv6 address 2001:DB8::1/32        ; Needed for IPv6.
     ipv6 enable           ; Needed for IPv6.
```

Step 2 Configure an 'ipv6 local pool' (used for AnyConnect Client IPv6 address assignment):

```
ipv6 local pool ipv6pool 2001:DB8:1:1::5/32 100     ; Use your IPv6 prefix here
```

Note You still need to configure an IPv4 address pool when using IPv6 (using the ip local pool command)

Step 3 Add the ipv6 address pool to your Tunnel group policy (or group-policy):

```
tunnel-group YourTunGrp1 general-attributes  ipv6-address-pool ipv6pool
```

Note Again, you must also configure an IPv4 address pool here as well (using the 'address-pool' command).

Step 4 Configure an IPv6 Tunnel Default Gateway:

```
ipv6 route inside ::/0 X:X:X:X::X tunneled
```

Enabling Modules for Additional AnyConnect Features

As new features are released for the AnyConnect client, you must update the AnyConnect clients of your remote users for them to use the new features. To minimize download time, the AnyConnect client requests downloads (from the security appliance) only of modules that it needs for each feature that it supports. To enable new features, you must specify the new module names using the **svc modules** command from group policy webvpn or username webvpn configuration mode:

[**no**] **svc modules** {**none** | **value** *string*}

Separate multiple strings with commas.

For a list of values to enter for each AnyConnect client feature, see the release notes for the Cisco AnyConnect VPN Client.

In the following example, the network administrator enters group-policy attributes mode for the group policy telecommuters, enters webvpn configuration mode for the group policy, and specifies the string vpngina to enable the AnyConnect client feature Start Before Login:

```
hostname(config)# group-policy telecommuters attributes
hostname(config-group-policy)# webvpn
hostame(config-group-webvpn)# svc modules value vpngina
```

Configuring, Enabling, and Using Other AnyConnect Features

The following sections describe how to configure other AnyConnect features. Some features, such as Secure Desktop and dynamic access policies, do not require that you specifically configure the AnyConnect client to interact with that feature. Rather, all configuration for those features occurs on the security appliance or within the software package itself.

Configuring Certificate-only Authentication

You can specify whether you want users to authenticate using AAA with a username and password or using a digital certificate (or both). When you configure certificate-only authentication, users can connect with a digital certificate and are not required to provide a user ID and password. To configure certificate-only authentication using the CLI, use the **authentication** command with the keyword **certificate** in tunnel-group webvpn mode. For example:

```
hostname(config)# tunnel-group testgroup webvpn-attributes
asa2(config-tunnel-webvpn)# authentication ?
asa2(config-tunnel-webvpn)# authentication certificate
```

Note You must configure **ssl certificate-authentication interface** <*interface*> **port** <*port*> for this option to take effect.

To configure certificate-only authentication using ASDM, select Configuration > Remote Access > Network (Client) Access > SSL VPN Connection Profiles, and in the Connection Profiles area, select Add or Edit. This displays the Add or Edit SSL VPN Connect Profile dialog box with the Basic option selected. In the Authentication area, specify only Certificate as the Method.

Using Compression

On low-bandwidth connections, compression increases the communications performance between the security appliance and the client by reducing the size of the packets being transferred. By default, compression for all SSL VPN connections is enabled on the security appliance, both at the global level and for specific groups or users. For broadband connections, compression might result in poorer performance.

Note the AnyConnect client for Windows Mobile does not support compression.

You can configure compression globally using the **compression svc** command from global configuration mode. You can also configure compression for specific groups or users with the **svc compression** command in group-policy and username webvpn modes. The global setting overrides the group-policy and username settings.

Changing Compression Globally

To change the global compression settings, use the **compression svc** command from global configuration mode:

compression svc

no compression svc

To remove the command from the configuration, use the **no** form of the command.

In the following example, compression is disabled for all SSL VPN connections globally:

```
hostname(config)# no compression svc
```

Changing Compression for Groups and Users

To change compression for a specific group or user, use the **svc compression** command in the group-policy and username webvpn modes:

svc compression {**deflate** | **none**}

no svc compression {**deflate** | **none**}

By default, for groups and users, SSL compression is set to *deflate* (enabled).

To remove the **svc compression** command from the configuration and cause the value to be inherited from the global setting, use the **no** form of the command:

The following example disables compression for the group-policy sales:

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# svc compression none
```

Note For compression to work, both the **compression svc** command (configured from global configuration mode) and the **svc compression** command (configured in group-policy and username webvpn modes) must be enabled. If *either* command is set to **none** or to the **no** form, compression is disabled.

Configuring the Dynamic Access Policies Feature of the Security Appliance

On the security appliance, you can configure authorization that addresses the variables of multiple group membership and endpoint security for VPN connections. There is no specific configuration of AnyConnect required to use dynamic access policies. For detailed information about configuring dynamic access policies, see *Cisco ASDM User Guide, Cisco Security Appliance Command Line Configuration Guide,* or *Cisco Security Appliance Command Reference.*

Cisco Secure Desktop Support

Cisco Secure Desktop validates the security of client computers requesting access to your SSL VPN, helps ensure they remain secure while they are connected, and attempts to remove traces of the session after they disconnect. The Cisco AnyConnect VPN Client supports the Secure Desktop functions of Cisco Secure Desktop for Windows 2000 and Windows XP. There is no specific configuration of AnyConnect required to use Secure Desktop. For detailed information about configuring Cisco Secure Desktop, see the *Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators (Software Release 3.2)*.

Enabling AnyConnect Rekey

Configuring AnyConnect Rekey specifies that SSL renegotiation takes place during rekey.

When the security appliance and the SSL VPN client perform a rekey, they renegotiate the crypto keys and initialization vectors, increasing the security of the connection.

To enable the client to perform a rekey on an SSL VPN connection for a specific group or user, use the **svc rekey** command from group-policy and username webvpn modes.

[**no**] **svc rekey** {**method {new-tunnel | none | ssl}** | **time** ***minutes***}

method new-tunnel specifies that the client establishes a new tunnel during rekey.

method none disables rekey.

method ssl specifies that SSL renegotiation takes place during rekey.

time *minutes* specifies the number of minutes from the start of the session or from the last rekey until the next rekey takes place, from 1 to 10080 (1 week).

In the following example, the client is configured to renegotiate with SSL during rekey, which takes place 30 minutes after the session begins, for the existing group-policy *sales*:

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-policy)# svc rekey method ssl
hostname(config-group-policy)# svc rekey time 30
```

Note The security appliance does not currently support inline DTLS rekey. The AnyConnect client, therefore, treats all DTLS rekey events as though they were of the new tunnel method instead of the inline ssl type.

Enabling and Adjusting Dead Peer Detection

Dead Peer Detection (DPD) ensures that the security appliance (gateway) or the client can quickly detect a condition where the peer is not responding, and the connection has failed.

Note When using the AnyConnect client with DTLS on security appliance, Dead Peer Detection must be enabled in the group policy on the ASA to allow the AnyConnect client to fall back to TLS, if necessary. Fallback to TLS occurs if the AnyConnect client cannot send data over the UPD/DTLS session, and the DPD mechanism is necessary for fallback to occur.

To enable DPD on the security appliance or client for a specific group or user, and to set the frequency with which either the security appliance or client performs DPD, use the **svc dpd-interval** command from group-policy or username webvpn mode:

svc dpd-interval {[**gateway** {*seconds* | **none**}] | [**client** {*seconds* | **none**}]}

no svc dpd-interval {[**gateway** {*seconds* | **none**}] | [**client** {*seconds* | **none**}]}

Where:

gateway seconds enables DPD performed by the security appliance (gateway) and specifies the frequency, from 30 to 3600 seconds, with which the security appliance (gateway) performs DPD.

gateway none disables DPD performed by the security appliance.

client *seconds* enable DPD performed by the client, and specifies the frequency, from 30 to 3600 seconds, with which the client performs DPD.

client none disables DPD performed by the client.

To remove the **svc dpd-interval** command from the configuration, use the **no** form of the command:

The following example sets the frequency of DPD performed by the security appliance to 30 seconds, and the frequency of DPD performed by the client set to 10 seconds for the existing group-policy *sales*:

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-policy)# svc dpd-interval gateway 30
hostname(config-group-policy)# svc dpd-interval client 10
```

Enabling AnyConnect Keepalives

You can adjust the frequency of keepalive messages to ensure that an AnyConnect client or SSL VPN connection through a proxy, firewall, or NAT device remains open, even if the device limits the time that the connection can be idle. Adjusting the frequency also ensures that the client does not disconnect and reconnect when the remote user is not actively running a socket-based application, such as Microsoft Outlook or Microsoft Internet Explorer.

To set the frequency of keepalive messages, use the **svc keepalive** command from group-policy webvpn or username webvpn configuration mode:

[**no**] **svc keepalive {none |** *seconds***}**

none disables client keepalive messages.

seconds enables the client to send keepalive messages, and specifies the frequency of the messages in the range of 15 to 600 seconds.

The default is keepalive messages are disabled.

Use the **no** form of the command to remove the command from the configuration and cause the value to be inherited:

In the following example, the security appliance is configured to enable the client to send keepalive messages with a frequency of 300 seconds (5 minutes), for the existing group-policy *sales*:

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# svc keepalive 300
```

Configuring Windows Mobile Support Using ASDM

You configure AnyConnect client Windows Mobile support just as you would any other Windows platform, with the following considerations:

- Windows Mobile connections require a special license, which you install just as you would any other AnyConnect client license. If you do not have this licensed installed, Windows Mobile connections do not work.
- See the latest version of *Release Notes for Cisco AnyConnect VPN Client* for detailed, current information about Windows Mobile device support.
- AnyConnect client Windows Mobile connections do not support compression.
- Windows Mobile connections can use the default profile values, but you can configure a profile that specifies mobile policy device lock parameters. See Configuring Windows Mobile Policy, page 4-22 for details on configuring the Windows Mobile parameters.

Note The AnyConnect client supports Mobile Device Lock on Windows Mobile 5.0, 5.0AKU2, and 6.0, but not on Windows Mobile 6.1.

- If you have configured a profile specifically for Windows Mobile, then use the **svc profiles** command in group policy webvpn or username attributes webvpn configuration mode to specify a client profile to download that has Windows Mobile parameters specified. For example, **svc profiles value mymobileprofile** directs the security appliance to download the profile mymobileprofile. If you specify the command **svc profiles none**, the security appliance does not download any profile.
- To specify an SSL VPN client package file that the security appliance expands in cache memory for downloading to remote PCs, use the **svc image** command in webvpn configuration mode. For mobile users, you can decrease the connection time of the mobile device by using the **regex** keyword with this command. When the browser connects to the security appliance, it includes the User-Agent string in the HTTP header. When the security appliance receives the string, if the string matches an expression configured for an image, it immediately downloads that image without testing the other client images.

SDI Token (SoftID) Integration

Cisco AnyConnect VPN Client, Release 2.1 and higher, integrates support for RSA SecurID client software running on Windows XP and Windows 2000 platforms. This support allows IT administrators to make strong authentication a convenient part of doing business. RSA SecurID software authenticators reduce the number of items a user has to manage for safe and secure access to corporate assets. RSA

SecurID Software Tokens residing on a remote device generate a random, one-time-use passcode that changes every 60 seconds. The term SDI stands for Security Dynamics, Inc. technology, which refers to this one-time password generation technology that uses hardware and software tokens.

Note The AnyConnect client is compatible with RSA SecurID software versions 1.1 and higher. At the time of this release, RSA SecurID Software Token client software does not support Windows Vista and 64-bit systems. In addition, the AnyConnect client does not support token selection from multiple tokens imported into the RSA Software Token client software. Instead, the AnyConnect client uses the default selected via the RSA SecurID Software Token GUI.

Comparing Native SDI with RADIUS SDI

The network administrator can configure the secure gateway to allow SDI authentication in either of the following modes:

- *Native SDI* refers to the native ability in the secure gateway to communicate directly with the SDI server for handling SDI authentication.
- *RADIUS SDI* refers to the process of the secure gateway performing SDI authentication using a RADIUS SDI proxy, which communicates with the SDI server.

In Release 2.1 and higher, except for one case, described later, Native SDI and RADIUS SDI appear identical to the remote user. Because the SDI messages are configurable on the SDI server, the message text (see Table 3-1 on page 3-18) on the security appliance must match the message text on the SDI server. Otherwise, the prompts displayed to the remote client user might not be appropriate for the action required during authentication. The AnyConnect client might fail to respond and authentication might fail.

RADIUS SDI challenges, with minor exceptions, essentially mirror native SDI exchanges. Since both ultimately communicate with the SDI server, the information needed from the client and the order in which that information is requested is the same. Except where noted, the remainder of this section deals with native SDI.

When a remote user using RADIUS SDI authentication connects to the security appliance with the AnyConnect VPN client and attempts to authenticate using an RSA SecurID token, the security appliance communicates with the RADIUS server, which in turn, communicates with the SDI server about the authentication.

For more information about configuring the ASA to ensure AnyConnect client compatibility, see Ensuring RADIUS/SDI Proxy Compatibility with the AnyConnect Client, page 3-15.

Using SDI Authentication

In releases of the AnyConnect client prior to Release 2.1, a user who wanted to use SecurID had to click Select in the AnyConnect login dialog box to select the server, start the RSA SecurID Software Token GUI, click or type a Personal Identification Number (PIN), click or type Enter, copy the generated passcode, paste the passcode into the password field in the AnyConnect dialog, click Connect in the AnyConnect dialog, and close the RSA SecurID token GUI.

In the AnyConnect client, Release 2.1 and higher, the login (challenge) dialog box changes to match the type of authentication configured for the tunnel group to which the user belongs. The input fields of the login dialog box clearly indicate what kind of input is required for authentication. Users who rely on username/password authentication see a dialog box like that in Figure 3-2.

Figure 3-2 Username/Password Authentication Login Dialog Box

For SDI authentication, the remote user enters a PIN (Personal Identification Number) into the AnyConnect client software interface and receives an RSA SecurID passcode. After the user enters the passcode into the secured application, RSA Authentication Manager validates the passcode and allows the user to gain access.

In AnyConnect Release 2.0, The field following the username field has the label “Password”.

Users who use RSA SecurID hardware or software tokens see input fields indicating whether the user should enter a passcode or a PIN, and the status line at the bottom of the dialog box provides further information about the requirements. The user enters a software token PIN or passcode directly into the AnyConnect user interface. See Figure 3-3 on page 3-12.

Figure 3-3 PIN and Passcode Dialog Boxes

The appearance of the initial login dialog box depends on the secure gateway settings: the user can access the secure gateway either through the main login page, the main index URL, or through a tunnel-group login page, a tunnel group URL (URL/tunnel-group). To access the secure gateway via the main login page, the “Allow user to select connection” check box must be set in the secure gateway SSL VPN Connection Profiles. In either case, the secure gateway sends the client a login page. The main login page contains a drop-down box in which the user selects a tunnel group; the tunnel-group login page does not, since the tunnel-group is specified in the URL.

Starting with AnyConnect Release 2.1, in the case of a main login page (with a drop-down tunnel-group list), the authentication type of the default tunnel group determines the initial setting for the password input field label. For example, if the default tunnel group uses SDI authentication, the field label is “Passcode”; but if the default tunnel group uses NTLM authentication, the field label is “Password”. In Release 2.1 and higher, the field label is not dynamically updated with the user selection of a different tunnel group. For a tunnel-group login page, the field label matches the tunnel-group requirements.

Also starting with AnyConnect Release 2.1, the client supports input of RSA SecurID Software Token PINs in the password input field. If the RSA SecurID Software Token software is installed and the tunnel-group authentication type is SDI, the field label is “Passcode” and the status bar states “Enter a username and passcode or software token PIN.” If a PIN is used, subsequent consecutive logins for the same tunnel group and username have the field label “PIN”. The client retrieves the passcode from the RSA SecurID Software Token DLL using the entered PIN. With each successful authentication, the client saves the tunnel group, the username, and authentication type, and the saved tunnel group becomes the new default tunnel group.

The AnyConnect client accepts passcodes for any SDI authentication. Even when the password input label is “PIN”, the user may still enter a passcode as instructed by the status bar. The client sends the passcode to the secure gateway as is. If a passcode is used, subsequent consecutive logins for the same tunnel group and username have the field label “Passcode”.

Categories of SDI Authentication Exchanges

All SDI authentication exchanges fall into one of the following categories:

- Normal SDI Authentication Login

- Normal login challenge
- New user mode
- New PIN mode
- Clear PIN mode
- Next Token Code mode

Normal SDI Authentication Login

A normal login challenge is always the first challenge. The SDI authentication user must provide a user name and token passcode (or PIN, in the case of a software token) in the username and passcode or PIN fields, respectively. The client returns the information to the secure gateway (central-site device), and the secure gateway verifies the authentication with the authentication server (SDI or SDI via RADIUS proxy).

If the authentication server accepts the authentication request, the secure gateway sends a success page back to the client, and the authentication exchange is complete.

If the passcode is not accepted, the authentication fails, and the secure gateway sends a new login challenge page, along with an error message. If the passcode failure threshold on the SDI server has been reached, then the SDI server places the token into next token code mode. See "Next Passcode" and "Next Token Code" Challenges, page 3-15.

New User, Clear PIN, and New PIN Modes

The PIN can be cleared only on the SDI server and only by the network administrator.

In the New User, Clear PIN, and New PIN modes, the AnyConnect client caches the user-created PIN or system-assigned PIN for later use in the "next passcode" login challenge.

Clear PIN mode and New User mode are identical from the point of view of the remote user and are both treated the same by the secure gateway. In both cases, the remote user either must enter a new PIN or be assigned a new PIN by the SDI server. The only difference is in the user response to the initial challenge.

For New PIN mode, the existing PIN is used to generate the passcode, as it would be in any normal challenge. For Clear PIN mode, no PIN is used at all for hardware tokens, with the user entering just a token code. A PIN Of eight consecutive zeros, "00000000", is used to generate a passcode for RSA software tokens. In either case, the SDI server administrator must inform the user of what, if any, PIN value to use.

Adding a new user to an SDI server has the same result as clearing the PIN of an existing user. In both cases, the user must either provide a new PIN or be assigned a new PIN by the SDI server. In these modes, for hardware tokens, the user enters just a token code from the RSA device. In either case, the SDI server administrator must inform the user of what, if any, PIN value to use.

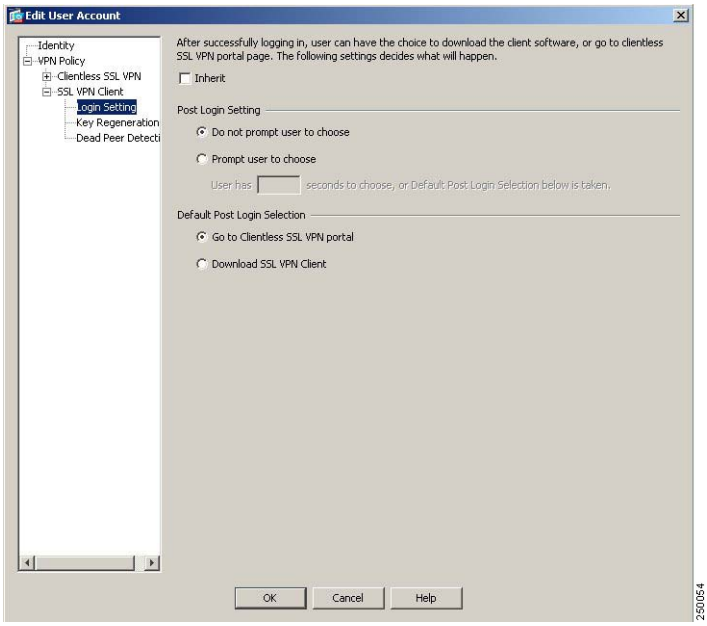
Getting a New PIN

If there is no current PIN, the SDI server requires that one of the following conditions be met, depending on how the system is configured:

- The user can choose whether to create a PIN or have the system assign it.
- The user must create a new PIN.
- The system must assign a new PIN to the user.

By default, the system simply assigns a PIN. If the SDI server is configured to allow the remote user to choose whether to create a PIN or have the system assign a PIN, the login screen presents a drop-down menu showing the options (Figure 3-4).

Figure 3-4 New PIN Creation or Generation Selection Dialog Box



The status line provides a prompt message. In either case, the user must remember the new PIN for future login authentications.

Creating a New PIN

If the user chooses to create a new PIN and clicks Continue, the AnyConnect client presents a dialog box on which to enter that PIN (Figure 3-5 on page 3-15). The PIN must be a number from 4 to 8 digits long.

Figure 3-5 Creating a New PIN

For a user-created PIN, after entering and confirming the new PIN, the user clicks Continue. Because the PIN is a type of password, anything the user enters into these input fields is displayed as asterisks. With RADIUS proxy, the PIN confirmation is a separate challenge, subsequent to the original dialog box. The client sends the new PIN to the secure gateway, and the secure gateway continues with a "next passcode" challenge.

For a system-assigned PIN, if the SDI server accepts the passcode that the user enters on the login page, then the secure gateway sends the client the system-assigned PIN. The user must click Continue. The client sends a response back to the secure gateway, indicating that the user has seen the new PIN, and the system continues with a "next passcode' challenge.

In both cases, the user must remember the PIN for subsequent login authentications.

"Next Passcode" and "Next Token Code" Challenges

For a "next passcode" challenge, the client uses the PIN value cached during the creation or assignment of a new PIN to retrieve the next passcode from the RSA SecurID Software Token DLL and return it to the secure gateway without prompting the user. Similarly, in the case of a "next Token Code" challenge for a software token, the client retrieves the next Token Code from the RSA SecurID Software Token DLL.

Ensuring RADIUS/SDI Proxy Compatibility with the AnyConnect Client

This section describes procedures to ensure that the AnyConnect client using RSA SecureID Software tokens can properly respond to user prompts delivered to the client through a RADIUS server proxying to an SDI server or servers. This section contains the following topics:

- AnyConnect Client and RADIUS/SDI Server Interaction

AnyConnect Client and RADIUS/SDI Server Interaction

When a remote user connects to the security appliance with the AnyConnect client and attempts to authenticate using an RSA SecurID token, the security appliance communicates with the RADIUS server, which in turn, communicates with the SDI server about the authentication.

During authentication, the RADIUS server presents access challenge messages to the security appliance. Within these challenge messages are reply messages containing text from the SDI server. The message text is different when the security appliance is communicating directly with an SDI server from when communicating through the RADIUS proxy. Therefore, in order to appear as a native SDI server to the AnyConnect client, the security appliance must interpret the messages from the RADIUS server.

Also, because the SDI messages are configurable on the SDI server, the message text on the security appliance must match (in whole or in part) the message text on the SDI server. Otherwise, the prompts displayed to the remote client user may not be appropriate for the action required during authentication. The AnyConnect client might fail to respond and authentication might fail.

Configuring the Security Appliance to Support RADIUS/SDI Messages

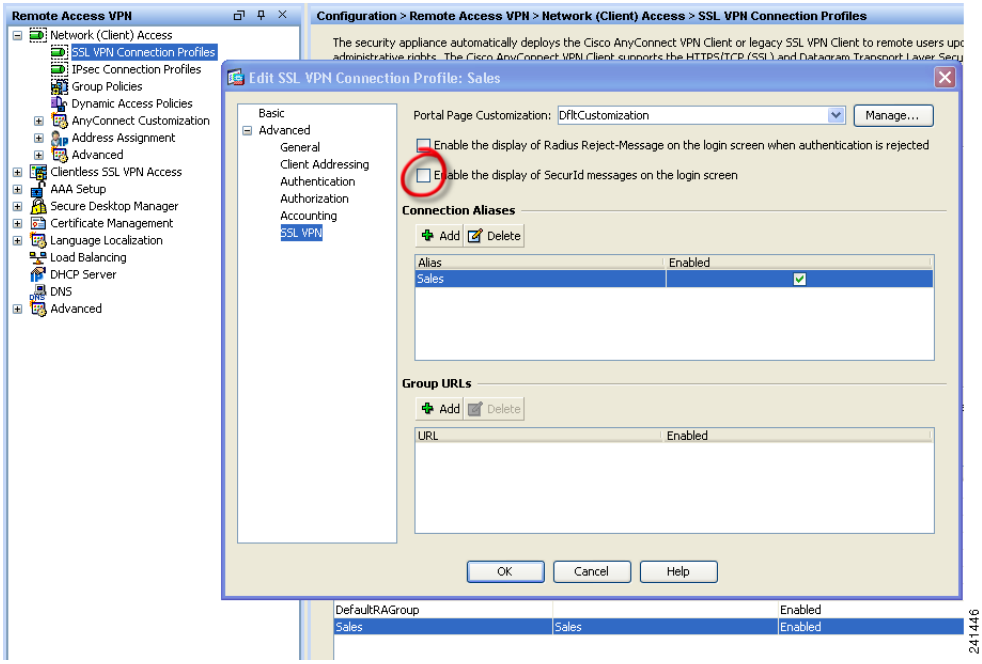
The following section describes the steps to configure the security appliance to interpret SDI-specific RADIUS reply messages and prompt the AnyConnect user for the appropriate action. Each step has information for both ASDM and the CLI.

Step 1 Configure a connection profile (tunnel group) to forward RADIUS reply messages in a manner that simulates direct communication with an SDI server. Users authenticating to the SDI server must connect over this connection profile.

ASDM Procedure

Go to Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles. The Edit SSL VPN Connection Profile window displays (Figure 3-6).

Figure 3-6 Edit SSL VPN Connection Profile Screen



Check **Enable the display of SecurID messages on the login screen**.

CLI Procedure

Use the **proxy-auth sdi** command from tunnel-group webvpn configuration mode. For example:

```
hostname(config)# tunnel-group sales webvpn attributes
hostname(tunnel-group-webvpn)# proxy-auth sdi
```

Step 2 Configure the RADIUS reply message text on the security appliance to match (in whole or in part) the message text sent by the RADIUS server.

The default message text used by the security appliance is the default message text used by Cisco Secure Access Control Server (ACS). If you are using Cisco Secure ACS, and it is using the default message text, you do not need to configure the message text on the security appliance. Otherwise, configure the messages to ensure the message text matches.

Table 3-1 shows the message code, the default RADIUS reply message text, and the function of each message. Because the security appliance searches for strings in the order in which they appear in the table, you must ensure that the string you use for the message text is not a subset of another string.

For example, “new PIN” is a subset of the default message text for both new-pin-sup and next-ccode-and-reauth. If you configure new-pin-sup as “new PIN”, when the security appliance receives “new PIN with the next card code” from the RADIUS server, it will match the text to the new-pin-sup code instead of the next-ccode-and-reauth code.

Table 3-1 SDI Opcodes, Default Message Text, and Message Function

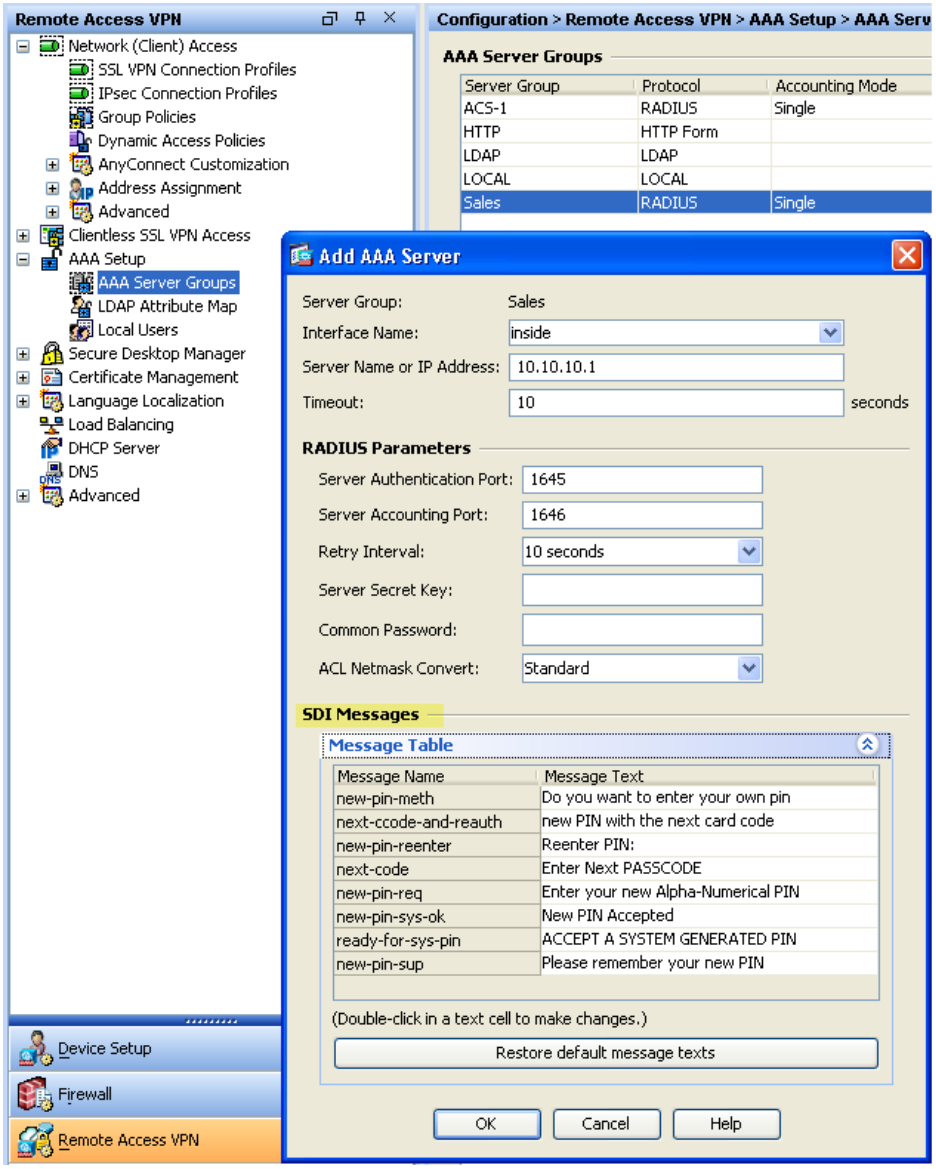
Message Code	Default RADIUS Reply Message Text	Function
next-code	Enter Next PASSCODE	Indicates the user must enter the NEXT tokencode without the PIN.
new-pin-sup	Please remember your new PIN	Indicates the new system PIN has been supplied and displays that PIN for the user.
new-pin-meth	Do you want to enter your own pin	Requests from the user which new PIN method to use to create a new PIN.
new-pin-req	Enter your new Alpha-Numerical PIN	Indicates a user-generated PIN and requests that the user enter the PIN.
new-pin-reenter	Reenter PIN:	Used internally by the security appliance for user-supplied PIN confirmation. The client confirms the PIN without prompting the user.
new-pin-sys-ok	New PIN Accepted	Indicates the user-supplied PIN was accepted.
next-ccode-and-reauth	new PIN with the next card code	Follows a PIN operation and indicates the user must wait for the next tokencode and to enter both the new PIN and next tokencode to authenticate.
ready-for-sys-pin	ACCEPT A SYSTEM GENERATED PIN	Used internally by the security appliance to indicate the user is ready for the system-generated PIN.

ASDM Procedure

Go to Configuration > Remote Access VPN > AAA Server Groups. The Add AAA Server window appears (Figure 3-7).

In the SDI Messages area, click Message Table to expand the table and view the messages. Double-click a message text field to edit the message.

Figure 3-7 Configuring RADIUS SDI Messages



CLI Procedure

Use the **proxy-auth_map sdi** command from tunnel-group webvpn configuration mode. The following example enters aaa-server-host mode and changes the text for the RADIUS reply message new-pin-sup:

```
hostname(config)# aaa-server radius_sales host 10.10.10.1
hostname(config-aaa-server-host)# proxy-auth_map sdi new-pin-sup "This is your new PIN"
```

Adding a Security Appliance to the List of Trusted Sites (IE)

See Adding a Security Appliance to the List of Trusted Sites (IE), page 2-18 for instructions about how to add a security appliance to the list of trusted sites. This is required on Windows Vista to use WebLaunch.